

Docket No.: 1509-281

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Marco Casassa MONT et al.

Serial No. Not yet assigned

Filed: herewith

For: DIGITAL CREDENTIAL MONITORING

Group Art Unit:

Examiner: N/A



CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Dear Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority
of:

United Kingdom Patent Application No. 0104078.1 filed February 20, 2001
of the present application.

The certified copy is submitted herewith.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe
Registration No. 19,641

Date: February 20, 2002
1700 Diagonal Road, Suite 310
Alexandria, Virginia 22314
Telephone: (703) 684-1111
Facsimile: (703) 518-5499
AML:EJ

THIS PAGE BLANK (USPTO)



INVESTOR IN PEOPLE

CERTIFIED COPY OF PRIORITY DOCUMENT

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

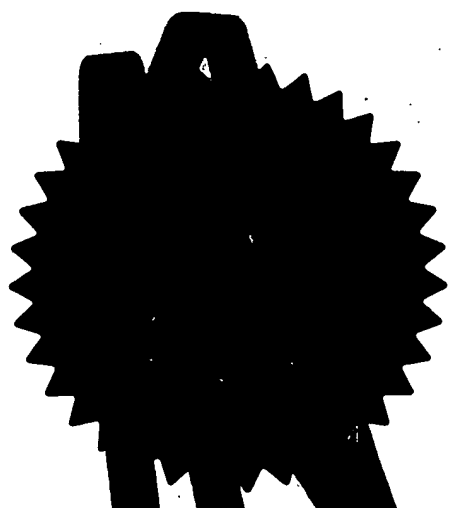


I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

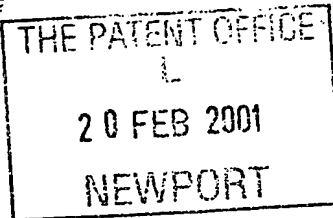
Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



Signed 

Dated 20 April 2001

THIS PAGE BLANK (USPTO)



The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

30007315 GB

1. Your reference

20 FEB 2001

0104078.1

2. Patent application number

(The Patent Office will fill in this part)

3. Full name, address and postcode of the or of each applicant (underline all surnames)

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

20FEB01 E607357-1 001463
P01/7700 0.00-0104078.1

Patents ADP number (if you know it)

Delaware, USA

496588004

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention Digital Credential Monitoring

5. Name of your agent (if you have one)

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

Richard A. Lawrence
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

7445035001

Patents ADP number (if you know it)

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country

Priority application number
(if you know it)

Date of filing
(day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:


Yes

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note (d))


Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description	24
Claim(s)	4
Abstract	1
Drawing(s)	8 + 8 

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent (Patents Form 7/77)	1 
Request for preliminary examination and search (Patents Form 9/77)	1
Request for substantive examination (Patents Form 10/77)	-

Any other documents
(please specify)

Fee Sheet

11.

I/We request the grant of a patent on the basis of this application.

Signature

Richard A. Lawrence

Date

19/2/01

12. Name and daytime telephone number of person to contact in the United Kingdom

Meg Joyce Tel: 0117-312-9068

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

30007315 GB

1

30007315

DIGITAL CREDENTIAL MONITORING

- 5 The present invention relates to the real time monitoring of digital credentials.

As the popularity of the internet has grown so has the number of internet services available on the internet, both at the business to consumer and business to business level.

10

However, an issue of concern to both consumers and businesses with respect to the provision of e-commerce and associated services is that of security and trust.

- 15 To help address this issue secure web protocols have been developed, for example the secure sockets layer (SSL) protocol. The security provisions provided by SSL include server authentication, client authentication, data integrity and confidentiality.

- 20 Authentication is provided by the exchange of digital certificates between the two users establishing a secure connection over the internet. The exchange of the digital certificates is an important process in the establishing of security and trust between two parties interacting on the internet. This is particularly so when the parties have never had any previous business interaction.

25

To provide confidence in the authentication process the digital identity certificates are issued by a trusted third party, for example Certification Authorities CA, who is responsible for managing the digital identity certificates life cycle.

30

The trusted third party monitors the status of a digital certificate. For example, the X.509 public key infrastructure (PKI) provides a check for the validity of X.509 certificates. This check, however, has to be done off-line. Therefore, a change in status of a digital certificate can not be monitored in real-time.

5

Current CA certificate management systems do not manage the real time "usage" of certificates at the application/service level, during active sessions within an enterprise. They are trust services external to the enterprise. They do not provide functionalities to an administrator to monitor the trustworthiness of digital credentials involved in active business transactions and tools to visualise aggregations of these certificates across multiple user web sessions

10

It is desirable to improve this situation.

15

In accordance with one aspect of the present invention there is provided a computer system comprising a first computer node coupled to a network, the first node being arranged to provide a service to a second computer node via a connection over the network; a controller for determining access to the service based upon a digital credential associated with the connection, the controller being arranged to vary access to the service over the connection in response to a change in status of the digital credential.

20

This provides the advantage of determining access to a service in 'real-time', thereby allowing a service level to be varied during a connection.

25

The term digital credential can include, identity certificate, attribute credential and anonymous credential.

30

Identity certificates are a collection of verifiable data containing information about the identity of entities, for example people, systems and applications.

X.509 identity certificates are currently the most popular certificates used on the internet. An X.509 identity certificate binds a name to a public key.

Attribute credentials are a collection of verifiable attributes and properties
5 associated to people, systems, applications and services.

Anonymous credentials contain attributes that are not associated to any identity credential, for example, electronic cash.

10 Therefore, users can analyse credentials to make decisions about the trustworthiness of the owners of the credentials.

Preferably the digital credential is an attribute credential of an entity associated with the second computer node.

15

Preferably the first computer node is arranged to provide the service to a plurality of computer nodes via a plurality of respective connections over the network.

20 Suitably the controller is suitable for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow a user to monitor the status of the digital credentials associated with a secure connection.

25 Preferably the computer system further comprising a digital register for listing the status of digital credentials; monitoring means for monitoring the digital register for changes in the status of a digital certificate, wherein the controller is responsive to the monitoring means for varying access to the service in response to a change in status of the digital credential.

30

In accordance with a second aspect of the present invention there is provided a computer node for providing a service to a second computer node via a

connection over a network, the computer node comprising a controller for determining access to the service based upon a digital credential associated with the connection, the controller being arranged to vary access to the service over the connection in response to a change in status of the digital credential.

10 In accordance with a third aspect of the present invention there is provided a controller for determining access to a service provided by a first computer node to a second computer node via a connection over a network, the controller being arranged to vary access to the service over the connection in response to a change in status of a digital credential associated with the connection.

15 In accordance with a fourth aspect of the present invention there is provided a method for providing a service, the method comprising establishing a connection between a first computer node and a second computer node via a network; providing a service for the second computer node from the first computer node via the connection; determining access to the service based upon a digital credential associated with the connection; varying access to the service over the connection in response to a change in status of the digital credential.

25 In accordance with a fifth aspect of the present invention there is provided a computer system comprising a first computer node coupled to a network, the first node being arranged to provide a service to a second computer node via a connection over the network; a controller for determining access to the service based upon a digital credential associated with the connection, the first node having memory for storing the digital credential associated with the connection and a display for presenting to a user information associated with the digital credential.

30

Preferably, the first node further comprises a controller for arranging digital credentials into groups, the groups being associated with a respective connection to allow a user to monitor digital credentials associated with a connection.

5

For a better understanding of the present invention and to understand how the same may be brought into effect reference will now be made, by way of one example only, to the accompanying drawings, in which:-

10 Figure 1 illustrates a computer system according to one embodiment of the present invention;

Figure 2 illustrates a computer system according to one embodiment of the present invention;

15

Figure 3 illustrates a computer node according to one embodiment of the present invention;

20 Figure 4 illustrates a user interface screen associated with one embodiment of the present invention;

Figure 5 illustrates a user interface screen associated with one embodiment of the present invention;

25 Figure 6 illustrates a user interface screen associated with one embodiment of the present invention;

Figure 7 illustrates a computer node according to one embodiment of the present invention;

30

Figure 8 illustrates a user interface screen associated with one embodiment of the present invention.

Figure 1 shows a first computer node 1 (which could be, for example, a single computer or a plurality of computers), connected to a second computer 2 (which could also be, for example, a single computer or a plurality of computers), via the internet 3. Both computer 1 and computer 2 have associated displays and keyboards, not shown. Also connected to the internet are certificate authorities, for example online certificate status protocol responder 4 OCSP, certificate verification server protocol responder 5 CVSP, certificate authorities CA 6 and attribute authorities 7 AA (for a description of these authorities see the internet engineering task force website www.ietf.org).

Computer 1 is arranged to support, typically, business or private users requiring services from a service provider on the internet 3, and as such includes a network protocol stack 8 including an internet browser 9 for browsing the internet, as is well known to a person skilled in the art. In addition to the browser 9 the protocol stack includes a 'browser plug in' 10 for handling trust related processes such as helping a user to explicitly manage the trustworthiness of digital credentials and pushing and pulling digital credentials during active internet sessions, as described below.

Computer 2 is arranged to support a service provider, typically an enterprise, for the provision of services to a client via the internet 3. Computer 2 incorporates a webserver 11 for providing web access to computer 2 for web clients, for example computer 1, as is well known to a person skilled in the art. In addition to a network protocol stack 12, computer 2 also includes a digital credential management system 13 for handling trust related processes, such as the management of large numbers of heterogeneous credentials in real time, as described below.

30

As computer 1 is arranged to support a user requiring a service, to aid clarity computer 1 will also, in this description, be referred to as user 1 to identify the

user, which could be a human operator or a software/hardware agent, of computer 1.

As computer 2 is arranged to support an enterprise providing an internet service, to aid clarity computer 2 will also, in this description, be referred to as enterprise 2 to identify the enterprise which could be a human operator or a software/hardware agent, of computer 2.

To enhance the level of security between a service provider using computer 2 and a web client using computer 1 a secure connection, for example a secure socket layer SSL connection, (i.e. a session) is established between computer 1 and the webserver 11 incorporated in computer 2, as is well known to a person skilled in the art. The SSL allows the authentication of users by the mutual transfer of digital identity certificates, the identity certificates being signed by a trusted third party such as a certificate authority CA 6, as is well known to a person skilled in the art. Once the users have been authenticated private keys are exchanged to allow encryption of data exchanged between the users.

To allow further analyses and managing, by the enterprise 2, of digital credentials (e.g. identity certificates, attribute credentials) associated with a session digital credentials are passed to a digital credential management system 14 at the enterprise side of the secure connection (i.e. computer 2).

The digital credential management system 14 is able to provide a full range of validation checks on the received digital credentials associated with a session according to a trust policy that is defined for the enterprise 2, for example by a computer administrator.

The validation checking of digital identity certificates associated with a session for the purposes of providing a service is defined as the user login phase. For this purpose the digital credential management system 14 incorporates a login

service module, as shown in figure 2, that interacts with a session manager module to create a new session object that is associated with a secure session, for its whole lifetime. The session object associates extra users' information to their session, for example bank statements associated to a user.

The login service module 16 retrieves the user's identity certificate from the web server 11 (used to establish the SSL session) and sends the certificate to a credential validation server module 17 for validation and trust management purposes.

The credentials validation server module 17 executes a two-phase control on the digital credential. First it performs "classic" verification tasks, like integrity and validation path checks. It interacts with external entities such as CA, OCSP and CVSP to check if the credential is still valid. OCSP and CVSP responders perform basic validation tasks on-line. Second, the module 17 determines the trustworthiness of the credential against explicit enterprise policies, for example checking explicit constraints on the validation path, on the issuer of the credentials, on the context in which the credential has been send.

Validation policies can be defined by an administrator and evaluated by an authorization server module 18, incorporated in the digital credential management system 14, thereby allowing the second task to be performed at runtime.

The authorization server module 18 interprets authorization and validation policies on the fly. Policies are loaded when the authorisation server module 18 starts up, along with the relevant models (service model, credential models, etc.). At any time policies and models can be modified and reloaded by the authorization server module 18 without service disruption. This

provides a high degree of freedom and flexibility to the administrator when dealing with trust management issues related to digital credentials.

5 If the digital credential under verification does not satisfy enterprise trust and validation policies, the credential is rejected and an error message is sent back to the user. If the digital credential satisfies enterprise policies, then it is passed to a credential content management module 19 where the digital credential is abstracted and its content analysed and managed according to enterprise policies. The credential validation server module manages the
10 interaction with the credential content manager module 19.

The digital credential content management module receives digital credentials from the credential validation server module 17 to perform further trust analysis on the credential content.

15 The credential content management module 19 abstracts a digital credential according to an abstraction model to remove the credentials dependency on its low-level format. This allows the abstracted credentials to be seen as a collection of attributes by the other validation and authorization framework
20 components, independently of their original representations.

The credential content management module 19 also manages the content of a digital credential according to trust and credential content management policies defined by the enterprise 2. These policies define which credential
25 components (attributes) need to be trusted, depending on their values, their issuers, the presence of other credentials, etc. The evaluation of these policies is delegated to the authorization server 18.

Every type of digital credential (identity, attribute and anonymous credential) is
30 subject to this process.

Once the digital credential has been abstracted and its content processed, the abstracted credential is returned to the credential validation server module 17.

5 The credential validation server module 17 is interfaced to a user context manager module 20, where the credential validation server module 17 forwards the abstracted digital credentials to the user context manager module 20. The user context manager module 20 stores the abstracted digital credentials into a user context area 21 associated with a user's session.

10 A user context area 21 contains all the relevant information known about a user during an active web session, for example user profile, roles and digital credentials.

The user context manager module 20 manages the user context areas 21 and
15 their associations to users' sessions, for the entire lifetime of these sessions.

The user context manager module 20 provides a set of application program interface's API to access the content of a specific user context area 21 at different levels of abstraction. It allows the retrieval of attributes independently
20 from their source (for example user profile, role and digital credential). In such a case it attaches to them metadata like their scope, qualifiers to allow analysis and evaluation by the authorisation server module 18.

When a new user context area 21 is created, the user context manager
25 module 20 retrieves from a database (not shown) of the enterprise 2 (service provider) relevant user information, like their profile and their roles and stores it in this user context. The stored information may have been obtained during previous transactions.

30 Each time the credential content management service module 19 successfully abstracts a user's credential, this credential is sent to the user context manager module 20 and stored in a user context area 21.

The user context manager module interacts with an object pool manager module 22 to dynamically manage the content of a user context.

- 5 Dynamic content management is useful as a particular role or a user profile could be valid just for a predefined period of time. Additionally a security administrator can modify the content of user profiles and roles at run time or during a user's session. Further, new digital credentials could be added to a user context area 21 during a user session and digital credentials could be
10 disabled/removed from a user context area 21 during a user session.

The ability to deal with these dynamic changes is important for the provision of real time authorization and access control service. The object pool manager module 22 is in charge of dynamically updating the content of user
15 contexts each time one of the above events occurs.

The user context manager module 20 supplies to a digital credentials usage monitoring service module 23 updated sets of active credentials (i.e. credentials that are currently used and enabled in a user context area and
20 digital credential usage monitoring service monitoring 23 executes the request of enabling/disabling credentials depending on trust and business management decisions.

The authorization server module 18 accesses a content of user contexts area
25 21 whilst evaluating policies. Policies may contain explicit constraints that need to be evaluated against the content of a user context area 21.

A user context gateway 24 manages the interaction between the user context manager module 20 and the digital credentials usage monitoring service
30 module 23. It provides a high-level application program interface API that can be used to access both user context manager module 20 and digital credentials usage monitoring service module 23 functionalities.

The user context gateway 24 acts as a gateway in the following cases; (i) when the user context manager module 20 sends to the digital credentials usage monitoring service module 23 an updated list of the digital credentials involved in active users' sessions; and (ii) when the digital credentials usage monitoring service module 23 asks the user context manager module 30 to enable/disable digital credentials, depending on trust and business management decisions.

- 10 Once user 1 has established a secure connection with enterprise 2 and has successfully completed the login phase and had their digital credentials validated by the enterprise 2, as described above, the enterprise 2 can provide a requested service over the secure session. Alternatively, before the service is provided the enterprise 2 may request the user to provide (push) further digital credentials (e.g. attribute credentials) in order to allow authorization to access services (i.e. to ensure that the enterprise has sufficient trust in the user).

20 User 1 can push an attribute credential to the enterprise 2 by using the browser plug-in 10, as described below. The browser plug-in 10 wraps a credential in a extended mark-up language XML message, contacts a credential proxy module 25 associated with the digital credential management system 14 in the enterprise/computer 2 and sends the message to the proxy module 25 over the secure connection.

25

The enterprise credential proxy module 25 is in charge of managing the push and pull process of attribute credentials.

30 During the push phase, the enterprise credential proxy module 25 extracts the attribute credential from the XML message and sends it to the enterprise credential validation server module 17 to be validated.

If the attribute credential is valid, it is sent to the credential content management service module 19 that abstracts it and sends it to the user context manager module 20.

- 5 The user context manager module 20 stores the digital credential in a user context area 21 associated with a relevant secure session and sends a copy of the credential to the credentials usage monitoring service module 23 to enable a real time monitoring of this credential.
- 10 User 1 can invoke the process of pushing a digital credential to the enterprise 2 at any time (and more than once) during an active user's session with the enterprise 2.

15 In addition the user 1 might want to obtain more information about an enterprise 2, before trusting its services and exposing their digital credentials to it. The user 1 may request the enterprise 2 to send them verifiable enterprise credentials containing trusted information (issued by a trusted third parties), about the way the enterprise operates, the quality of its services, references, etc.

20

Further, the enterprise 2 (or an entity on its behalf) can issue and send new digital credentials to user 1, which will be owned by the user. For example, where a bank sends digital statements to users containing information about their accounts. These user's credentials can enable further business
25 transactions with other enterprises.

To request a digital credential (i.e. pull) from enterprise 2, user 1 sends a XML message to the enterprise 2 to request digital credentials. This message could contain a request to obtain enterprise's credentials or to collect new user's
30 credentials. The request process can be very simple low level communication

and request mechanisms can be made transparent to the user. The messages are sent via the associated secure connection.

5 The enterprise credential proxy module 25 intercepts the user's request message and interprets it. If the request is valid, the proxy module 25 interacts with a credential issuer/pusher module 26.

10 The credential issuer/pusher module 26 is responsible for sending the enterprise's credentials to user 1 over the secure session, after verifying if the user 1 is entitled to receive the credentials. In order to do this, it interacts with the authorization server module 18 to evaluate proper policies based on the content of the current user context area 21. The enterprise credentials are sent to the credential proxy module 25, which wraps the credentials in another XML message and sends the message to the user 1.

15 In addition the credential issuer/pusher module 26 also sends new user's credentials to user 1 over a secure session. This allows new credentials to be issued to user 1 in real time. The issuer of these credentials can be the module 26 itself or an external attribute authority. New digital credentials can be associated to the current user's identity or they can be anonymous. The
20 module 26 verifies if the remote user is entitled to receive the new credentials. These new digital credentials are sent to the credential proxy module 25, which wraps the message in a XML message and sends it to the user over the secure connection.

25 The process of pulling digital credentials from enterprise 2 can happen at any time and more than once during an active user's session with the enterprise 2.

30 The process of exchanging credentials over a secure connection, as described above, can be used to establish trust or to increase the level of trust between two parties during business interactions. This enhances the process

of providing services over the internet with customers that you have had no previous business relationship.

This embodiment allows authorization policies to be associated to a service
5 where the policies can be defined in a service model. If the authorization
policies are defined in a service model the authorization server module 18
loads the service model at start time (i.e. when authorization server module
18 is 'booted up'). Should the policies in the service model be modified, the
authorization server module 18 can reload them at any time, without any
10 service disruption.

In this embodiment, authorization is driven by policies. Depending on the
service and the service functions a user wants to access, the authorization
server module 18 is able to retrieve the correct set of authorization policies
15 and evaluate them.

Different policy evaluation strategies can apply, so for example, if at least one
relevant policy is satisfied, the authorization is granted and the service is
provided.

20 Whilst making authorization decisions, the authorization server module 18 can
access a broad range of information. For example, service function
information; service parameters; system information, like time, date, external
access control information; and the content of the user context area 21
25 associated to the user in the current session: user profile, user's roles, user's
digital credentials.

As stated above the management of digital credential on the user side is
based on a browser plug-in 10 able to exchange credentials with enterprise 2
30 by using an XML based protocol. XML is used because ease and simplicity of
use, however other languages may be used, for example HTML.

As shown in figure 3 the browser plug-in 10 includes a XML-based protocol handler module 28, a sender/importer modules 29,30, a cache 31, a loader module 32, credential storage 33, a graphical user interface module 34 and pluggable modules 35.

5

The XML-based protocol handler module 28 manages incoming and outgoing XML messages. It implements an interpreter of the XML protocol to deal with the push and pulling of messages.

- 10 The protocol consists of three XML messages, an INIT, a PUSH and PULL message.

The INIT message is a message containing initialisation information for the browser plug-in and includes the URL of the credential proxy module 25; and
15 filtering information on digital credentials that can be sent by enterprise 2 to the user 1 (based, for example, on the credential issuer and signer).

The PUSH message contains one or more digital credentials sent by the user 1 to the enterprise.

20

The PULL message contains one or more digital credentials sent by the enterprise 2 to the user 1.

- 25 As the XML messages are exchanged on a secure connection (based on SSL) the messages do not need to be signed.

The sender/import modules 29, 30 are in charge of dealing with the process of pushing and pulling digital credentials.

- 30 The import module 30 extracts and manages digital credentials that have been sent to the user 1 by enterprise 2. In particular it manages attribute credentials pushed by the enterprise 2. These credentials could belong to the

enterprise 2 (to increase the level of trust) or to the user 1 (new attribute credentials associated to the user). The import module 30 is able to discriminate between the above two cases and associate credentials to the right owner. The import module 30 interacts with external pluggable modules
5 35 (described below) to verify the trustworthiness of digital credentials and store them. The import module 30 is driven by the graphical user interface module 34.

The sender module 29 deals with digital credentials that have been sent by
10 the user 1 to enterprise 2. It verifies if the selected attribute credentials can be pushed to the enterprise 2 by analysing the current context (e.g. user's identity certificate, association of attribute credentials to this identity, etc.) The sender module 29 creates the XML messages that are going to be pushed to the enterprise 2. The sender module 29 is driven by the graphical user
15 interface module 34.

The cache 31 is a volatile cache to store digital credentials involved in web sessions. These credentials may belong to the user 1 or the enterprise 2. Part of the cache memory is used to store the set of trusted CA roots (used for
20 trust verification) retrieved from the credential storage 33.

The loader module 32 loads X.509 identity certificates from the credential storage 33, which includes trusted root CA certificates. These certificates are used for credential validation purposes.

25

The pluggable modules 35 are external to the browser plug-in 10. They provide core functionalities in term of credential management, for example validation, verification, storage. These modules 35 are plugged-in in the browser plug-in 10. This approach provides freedom to use proper and ad-hoc
30 validation and storage solutions. User can implement their own ad-hoc validation and storage modules according to their requirements.

The credential storage 33 is a secure storage for attribute credentials. While identity certificates (X.509 based) are stored in the credential storage 33, digital signed XML attribute credentials are explicitly stored and secured in a separate database.

5

The graphical user interface module 34 is arranged to allow the credential information to be displayed on the display (not shown) and for user 1 to manage the secure sessions, thereby allowing the overall user experience to be simplified when dealing with digital credentials and associated management of trust.

10

The graphical user interface module 34 can arrange the whole set of digital credentials exchanged and involved in an active web session between a user 1 and a enterprise 2 to be displayed. For example, identity certificates and attribute credentials pushed by the user 1 to the enterprise 2; and identity certificates and attribute credentials owned by the enterprise 2 and pushed by enterprise 2 to the user 1.

15

The graphical user interface module 34 can be configured to automatically notified user 1 when a new digital credential has been sent to user 1. The user 1 can accept or reject a credential after the trust verification and validation processes (automatically executed by the system).

20

During a web session, the graphical user interface module 34 manages and checks the associations between attribute certificates and the legitimate identity certificates. In particular, this control is performed on incoming digital credentials. The graphical user interface module 34 automatically rejects attribute credentials that are not trusted or do not relate to any of the identity certificates used in the current session.

25

30

The graphical user interface module 34 dynamically manages the portfolio of active user's credentials. The graphical user interface module 34 can be

configured to just present to the user 1 the list of attribute certificates the user 1 is entitled to push to the enterprise 2 (set of attribute certificates associated to the current identity).

- 5 Pushing a credential to the enterprise 2, from the users perspective, can simply be the dragging and dropping of an attribute credential in a session box (i.e. the graphic box on the display that represents the secure connection).
- 10 Figures 4 illustrates an example of a possible user interface screen. The top left panel of the user interface screen, shown in figure 4, displays the updated set of digital credentials that have been exchanged during an active session both by the user 1 and the enterprise 2. This panel contains a reference to the identity certificate used by the user 1 to establish the SSL connection and any
- 15 attribute credentials that may have been transferred over the SSL connection.

The bottom left panel of the user interface screen, shown in figure 4, provides information about user's credentials. In particular it displays only the attribute credentials that are associated to the current identity certificate.

20

The user can exchange any of their credentials by selecting the appropriate credential and drag and dropping it in the "Session" panel.

- Figure 5 shows a view of the user interface screen after the user has pushed
- 25 a citizenship credential.

The user interface panels can display both user's credentials and the credentials exchanged by with enterprise 2.

- 30 Figure 6 shows a user interface screen displaying the contents of an attribute credential provided by a market maker to the user. The attributes contained in the credential can be relevant to increase the perception of trust. For

example, the attribute credential shown in figure 6 shows that the market maker is compliant with the security and audit requirements:

5 A user can administer at any time its current portfolio of digital credentials, even when they are no active sessions.

The corresponding module on the enterprise 2 for handling the XML-based messages during an active secure session is the credential proxy server module 25.

10

As described above the credential proxy server module 25 receives messages containing digital credentials sent by the user to the enterprise 2. It extracts these credentials from the XML message and sends the credentials to the validation server module 17, which validates the certificates and adds them to
15 the appropriate user context area 21.

Digital credentials to be sent by the enterprise 2 to user 1 are forwarded to the credential proxy server module 25. The credential proxy server module 25 wraps the digital credentials in a XML message and sends the message to the
20 user's browser plug-in 10 when required over the secure session.

To provide real time status of a digital credential the credential usage monitoring service module 23 implements a real time monitoring system for digital credentials presented by user 1 to enterprise 2, during an active web
25 sessions, as described below.

This credential usage monitoring service module 23 is able to deal with real time, session-based credential validation and aggregation. The module 23 can provide different views on set of credentials to a security administrator
30 and tools for validating credential trustworthiness against enterprise policies.

In addition the credential usage monitoring service module 23 can retrieve active digital credentials from the user context manager module 20 and aggregates them according to views required by the security administrator.

- 5 Examples of views supported by the credential usage monitoring service module 23 are; aggregation of attribute credentials and identity certificates in the context of a web session (between user 1 and the enterprise 2); aggregation of attribute credentials and identity credentials depending on the presence of specific attributes. For example credentials can be aggregated
10 depending on the name of the company the owner of a credential works for or the name of a particular attribute (Credit Limit, Citizenship, etc.).

Further the credential usage monitoring service module 23 can provide a dynamic control over the usage of digital credentials at the service level.

15

- For example an administrator can verify the validity of digital credentials using the credential usage monitoring service module 23 to interact with the validation service module 17 (driven by policies) or external validation mechanisms. Also an administrator can enable or disable users' credentials in
20 real time. The credential usage monitoring service module 23 can interact with the user context manager module 20 to update its content.

- As shown in figure 7, the credential usage monitoring service manager 23 includes an object manager module 36, a session cache manager module 37,
25 a data model module 38, an aggregation module 39, a credential usage control module 40 and a graphical user interface module 41.

- The object manager module 36 acts as a proxy between the user context gateway module 24 and the session cache manager module 37. The object
30 manager module 36 retrieves credentials contained in active user contexts areas 21 and the list of active users' sessions. The module 36 then provides this information to the session cache manager module 37. Should the status

of a credential change, the module will communicate this change to the user context manager 20.

5 The session cache manager module 37 caches information about the current set of active sessions and their associations to digital credentials. The session cache manager module 37 provides the cached data to the data model module 38.

10 The data model module 38 contains information relating to how to interpret the content of digital credentials associated to sessions and how to represent them graphically.

15 The aggregation module 39 implements functions to aggregate digital credentials depending on administrator's queries and selection criteria. These criteria could involve the content of digital credentials, value of particular attributes, association constraints, etc.

20 The credential usage control module 40 controls the validity and trustworthiness of digital credentials associated to active sessions whilst they are used to access services. The control is driven by enterprise policies. The credential usage control module 40 retrieves the set of credentials and sessions to be controlled from the aggregation module 39.

25 The most common controls performed on credentials include, checking the validity of credentials, verifying their trustworthiness against enterprise policies, verifying the validity of associations of attributes credentials with identity certificates.

30 The credential usage control module 40 can execute these controls in a programmable way. The controls can be scheduled and done periodically, each time a new credential is added or driven by administrator's initiatives.

The credential usage control module 40 notifies the object manager module 36 of any change of digital credential statuses.

5 An administrator can access the functionalities of the credential usage control module 40 by using a user interface associated with enterprise 2 via the graphical user interface 41.

The graphical user interface module 41 implements the graphical routines, which are accessible to an administrator by the user interface.

10

The graphical user interface module 41 generates user interface screens for display on a display (not shown),

15 The user interface screens simplifies the overall interaction of an administrator with the credential usage monitoring service module 23 by providing an abstract graphical representation of digital credentials and relationships among them.

20 The user interface screens display aggregations and views on digital credentials in an intuitive way and allows the administrator to easily access tools to manage the validity and trustworthiness of digital credentials.

The user interface screens can provides a list of all the active user contexts areas associated to user web sessions. The list can be updated dynamically,
25 in real time.

An administrator can select or look for a set of credentials and execute operation on it (enable, disable and verification).

30 Figures 8 illustrate an example of a possible user interface screen. The top panel of the user interface screen, shown in figure 9, contains information about the current set of active contexts (active context list), each of them

associated to an active user session. As the enterprise 2 is able to establish a plurality of secure connections with different users, at the same time, the interface screen is arranged to display each active user session.

- 5 Each row shown in the top panel of figure 8 is an abstraction of an active user context and it contains references to the associated identity and attribute credentials. The contents of this display are updated in real time each time new users log in, exit their connections or push new credentials.
- 10 The user interface allows an administrator to select rows or a sub set of them and apply search criteria. The user interface can be used to define search and grouping criteria for credentials.

- The user interface can allow the administrator to directly intervene on
- 15 credentials and change their status in real time.

CLAIMS

1. A computer system comprising a first computer node coupled to a network, the first node being arranged to provide a service to a second computer node via a connection over the network; a controller for determining access to the service based upon a digital credential associated with the connection, the controller being arranged to vary access to the service over the connection in response to a change in status of the digital credential.
2. A computer system according to claim 1, wherein the controller forms part of the first computer node.
3. A computer system according to claim 1 or 2, wherein the digital credential is an attribute credential of an entity associated with the second computer node.
4. A computer system according to any preceding claim, wherein the first computer node is arranged to provide the service to a plurality of computer nodes via a plurality of respective connections over the network.
5. A computer system according to claim 4, wherein the controller is suitable for arranging digital credentials into groups, each group being associated with one or more respective secure connections to allow a user to monitor the status of the digital credentials associated with a secure connection.
6. A computer system according to claim 4 or 5, wherein the controller is suitable for arranging digital credentials into groups, each group being associated with one or more respective secure connections to allow the controller to control the digital credentials according to a policy.

- 5 7. A computer system according to any preceding claim, further comprising a digital register for listing the status of digital credentials; monitoring means for monitoring the digital register for changes in the status of a digital credential, wherein the controller is responsive to the monitoring means for varying access to the service in response to a change in status of the digital credential.
- 10 8. A computer system substantially as hereinbefore described with reference to the accompanying drawings.
- 15 9. A computer node for providing a service to a second computer node via a connection over a network, the computer node comprising a controller for determining access to the service based upon a digital credential associated with the connection, the controller being arranged to vary access to the service over the connection in response to a change in status of the digital credential.
- 20 10. A computer node according to claim 9, wherein the service is provided to a plurality of computer nodes via a plurality of respective connections over the network.
- 25 11. A computer node according to claim 10, wherein the controller is suitable for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow a user to monitor the status of the digital credentials associated with a secure connection.
- 30 12. A computer node according to claim 10 or 11, wherein the controller is suitable for arranging digital credentials into groups, the groups being associated with a respective secure connection to allow the controller to control the digital credentials according to a policy.

13. A computer node substantially as hereinbefore described with reference to the accompanying drawings.

5 14. A controller for determining access to a service provided by a first computer node to a second computer node via a connection over a network, the controller being arranged to vary access to the service over the connection in response to a change in status of a digital credential associated with the connection.

10 15. A method for providing a service, the method comprising establishing a connection between a first computer node and a second computer node via a network; providing a service for the second computer node from the first computer node via the connection; determining access to the service based upon a digital credential associated with the
15 connection; varying access to the service over the connection in response to a change in status of the digital credential.

20 16. A method for providing a service substantially as hereinbefore described with reference to the accompanying drawings.

25 17. A computer system comprising a first computer node coupled to a network, the first node being arranged to provide a service to a second computer node via a connection over the network; a controller for determining access to the service based upon a digital credential associated with the connection, the first node having memory for storing the digital credential associated with the connection and a display for presenting to a user information associated with the digital credential.

30 18. A computer system according to claim 17, wherein the first node further comprises a controller for arranging digital credentials into groups, the

30007315 GB

28

groups being associated with a respective connection to allow a user to monitor digital credentials associated with a connection.

ABSTRACT**DIGITAL CREDENTIAL MONITORING**

5

A computer system comprising a first computer node coupled to a network, the first node being arranged to provide a service to a second computer node via a connection over the network; a controller for determining access to the service based upon a digital credential associated with the connection, the
10 controller being arranged to vary access to the service over the connection in response to a change in status of the digital credential.

15 (Figure 2)

THIS PAGE BLANK (USPTO)

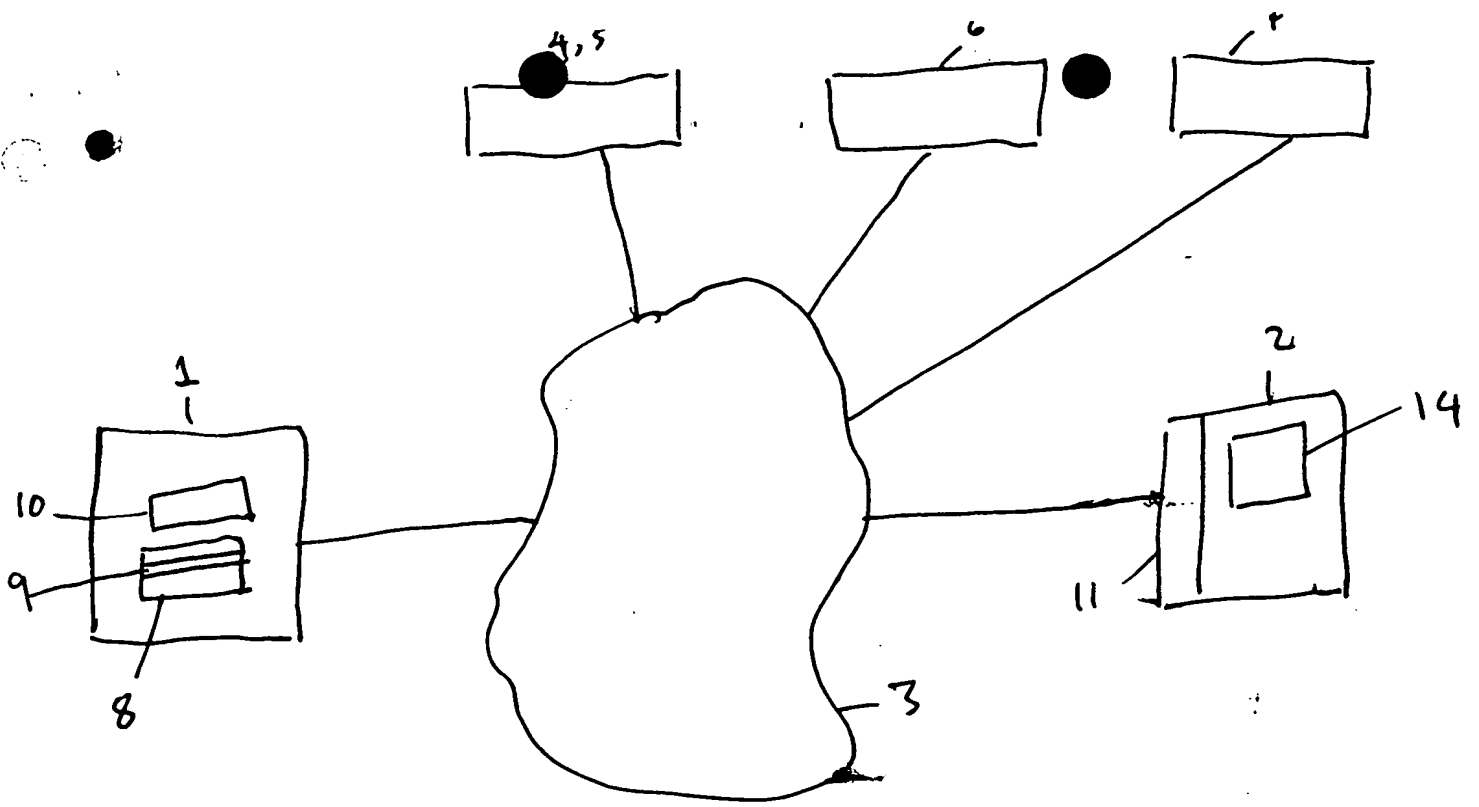


Fig 1

THIS PAGE BLANK (USPTO)

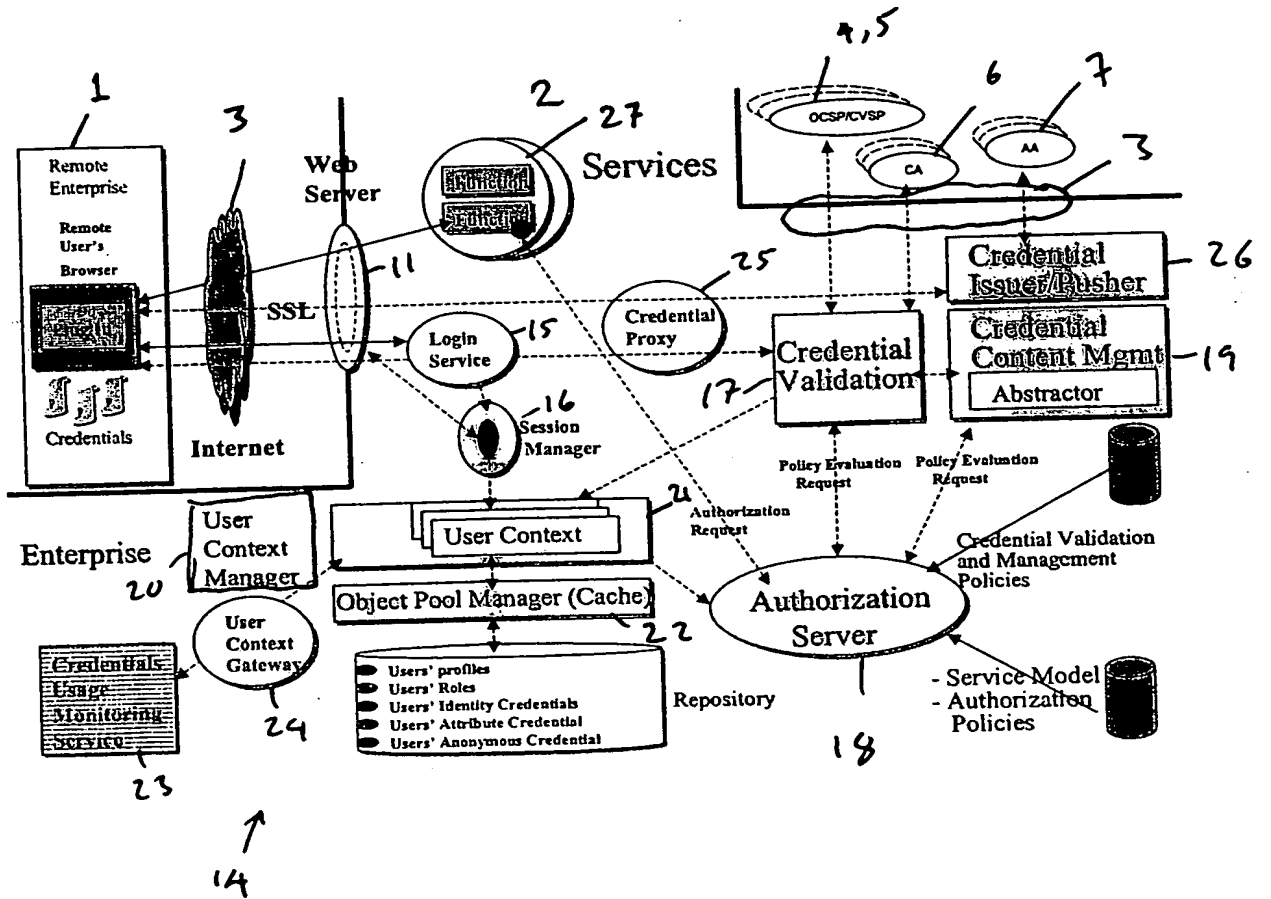


Fig 2

THIS PAGE BLANK (USPTO)

Best Available Copy

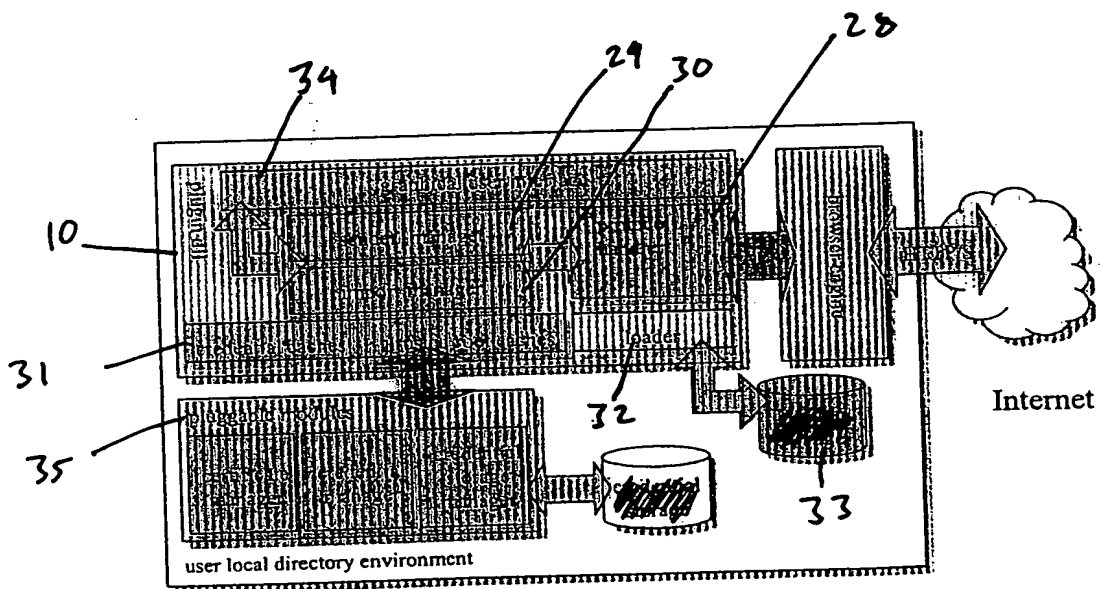


Figure 3

THIS PAGE BLANK (USPTO)

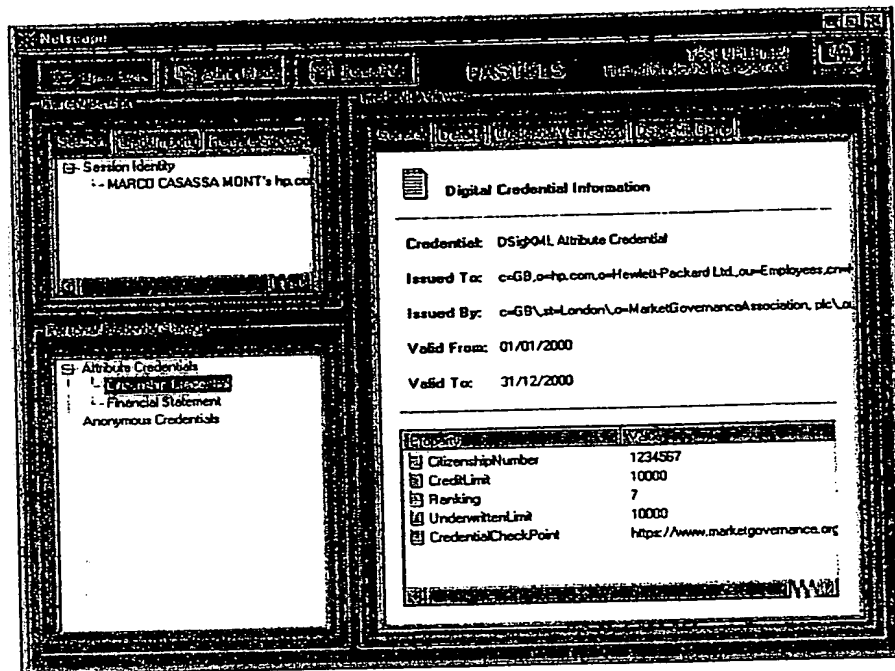


Figure 4

NOT PAGE BLANK (USPTO)

Best Available Copy

Session Identity

MARCO CASASSA MONT's hp.co

Page 1 of 1

http://www.marco-casassa.com/

Figure 5

THIS PAGE BLANK (USPTO)

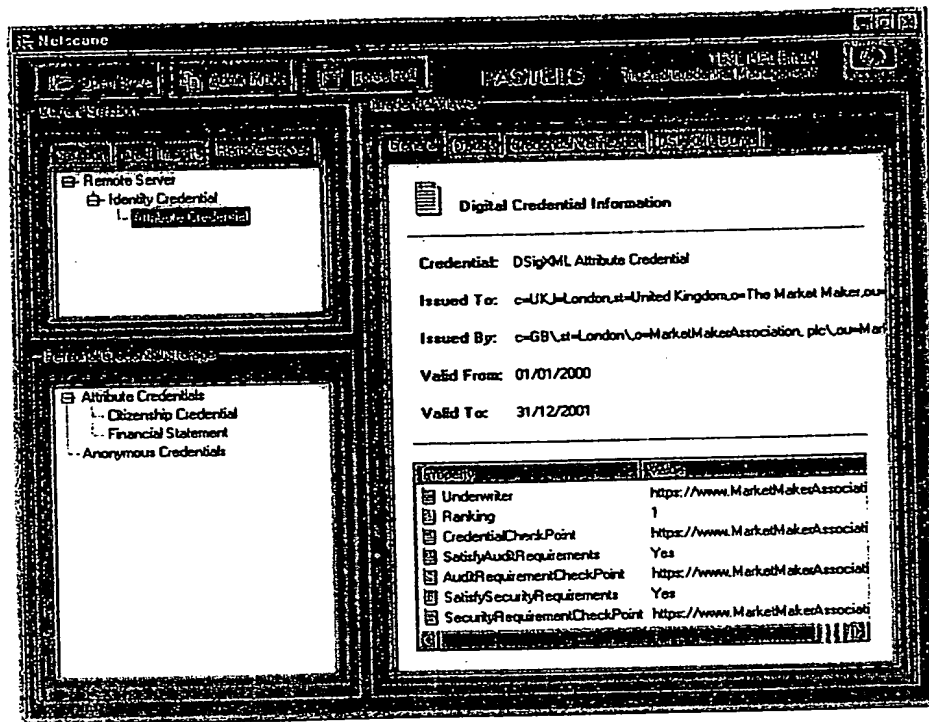


Figure 6

THIS PAGE BLANK (USPTO)

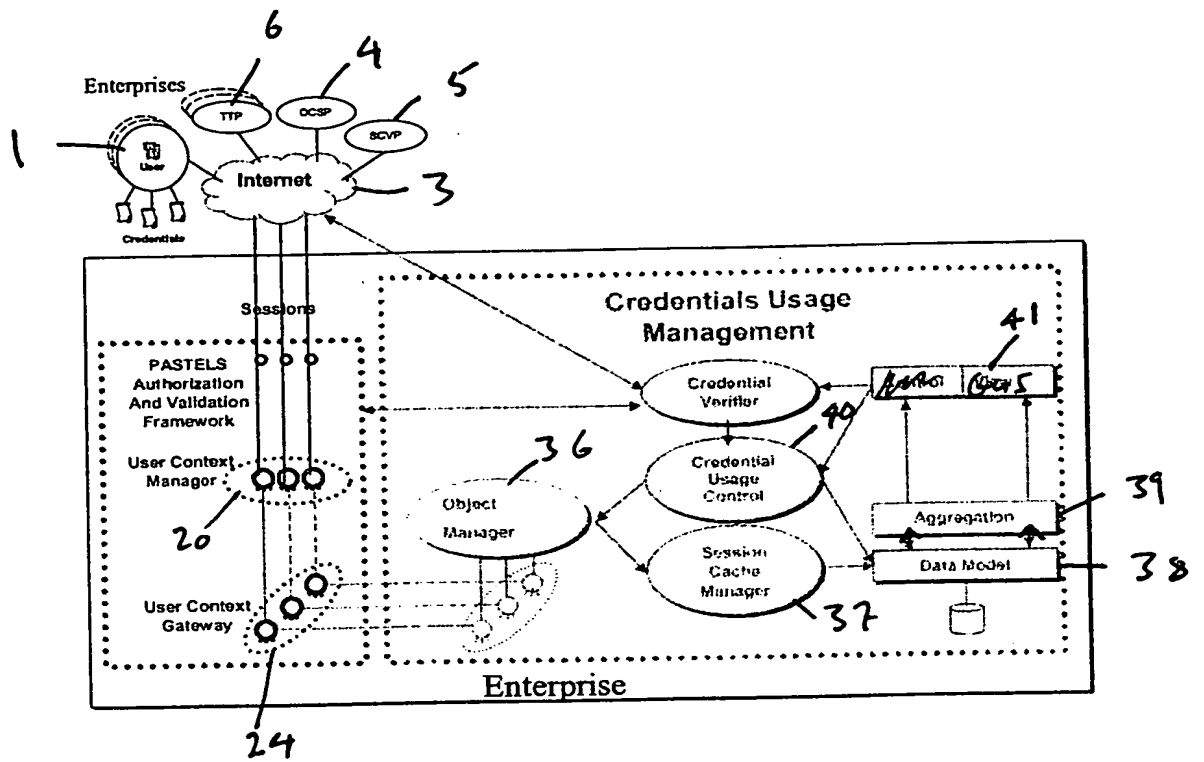


Figure 7

THIS PAGE BLANK (USPTO)

Trustview - Credentials Usage Monitor					
Filter: All					
Source	Destination	Source	Destination	Status	Splice
0	cn=Stephen Dior	cn=Robert Palmer	cn=Robert Palmer	OK	
8	cn=Robert Palmer	cn=Madeline Orbright	cn=Madeline Orbright	OK	
7	cn=Madeline Orbright	cn=Kathy Orange	cn=Kathy Orange	OK	
6	cn=Kathy Orange	cn=Jim Morrison	cn=Jim Morrison	OK	
5	cn=Jim Morrison	cn=Jason Bronson	cn=Jason Bronson	OK	
4	cn=Jason Bronson	cn=Tad Lee-Van	cn=Tad Lee-Van	OK	
10	cn=Tad Lee-Van	cn=Gerald Hallwell	cn=Gerald Hallwell	OK	
3	cn=Gerald Hallwell	cn=Darren Halloway	cn=Darren Halloway	OK	
2	cn=Darren Halloway	cn=Andrew Lee	cn=Andrew Lee	OK	
1	cn=Andrew Lee	cn=Alice Andersen	cn=Alice Andersen	OK	
0	cn=Alice Andersen				

<p>Filter: All</p> <p>Source: cn=Stephen Dior</p> <p>Destination: cn=Robert Palmer</p> <p>Status: OK</p> <p>Splice: </p>	<p>CREDENTIAL INFORMATION</p> <p>Issued to: Stephen Dior</p> <p>Issued by: MarketOovernanceAssociation Citizen Manager Signer</p> <p>Valid from: Sat Jan 01 00:00:00 GMT 2000 to Sun Dec 31 00:00:00 GMT 2000</p> <p>Credit Limit: 20000</p>
--	--

IDENTITY CREDENTIALS grouped by ISSUER DN

- cn=UK
 - cn=London
 - cn=United Kingdom
 - cn=Verisign
 - cn=Trust Services
 - cn=The Verisign CA
 - CONTEXT - ContextID=9
 - IDENTITY CREDENTIAL - cn=Stephen Dior
 - ATTRIBUTE CREDENTIAL - cn=Stephen Dior

Figure 8

THIS PAGE BLANK (USPTO)